導入の計画

プランニング ワークフロー

次の表に、アプライアンスの設置、設定、およびセットアップを試みる前に実行する必要がある計画および情報収集タスクの詳細を示します。この表のタスクが完了したら、データセンターにアプライアンスを物理的に設置することで続行できます。

詳細については「Cisco DNA CenterおよびCisco Software-Defined Access」を参照してください。

表 *1:* 計画作業

ステップ	説明
1	スタンドアロン設置およびクラスタ設置で推奨されるケーブル接続とスイッチングの要件を確認します：インターフェイスケーブル接続。
2	アプライアンスの設定時に適用する IP アドレッシング、サブネット化、およびその他の IP トラフィック情報を収集します：必要な IP アドレスおよびサブネット。
3	Web ベースのリソースへのアクセスに必要なソリューションを準備します：必要なインターネット URL と完全修飾ドメイン名、インターネットへのアクセスを保護。

ステップ	説明
4	Cisco DNA Center トラフィックのファイアウォールおよびセキュリティポリシーを再設定します：必要なネットワークポート。Cisco DNA Center を使用して SDA ネットワークを管理している場合は、「必要な SD アクセス ポートおよびプロトコル」も参照してください。
5	アプライアンスの設定時および初回のセットアップ時に使用される追加情報を収集します：必須の設定情報と必要な初期設定情報。

Cisco DNA CenterおよびCisco Software-Defined Access

Cisco SD-Access ファブリックアーキテクチャを使用するネットワークも含め、すべてのネットワークタイプで Cisco DNA Centerを使用できます。Cisco SD-Accessは、従来のネットワークをインテントベースのネットワークに変換します。これにより、ビジネスロジックがネットワークの物理的な部分になり、構成、プロビジョニング、トラブルシューティングなどの日常的なタスクを簡単に自動化できるようになります。Cisco SD-Access ソリューションは、ネットワークをビジネスニーズに合わせ、問題解決を改善し、セキュリティ侵害の影響を軽減するために必要な時間を短縮します。

Cisco SD-Access ソリューションの詳細については、このガイドの範囲外です。Cisco DNA Center で使用する Cisco SD-Access ファブリックアーキテクチャの実装を計画しているネットワークアーキテクトや管理者は、次のリソースから追加情報とガイダンスを入手できます。

- 通常のネットワークのアプローチと技術では不可能なソリューションを自動化するために、Cisco DNA Center が Cisco SD-Access を活用する方法については、『ソフトウェア定義型アクセス：インテントベースのネットワーキングの実現』を参照してください。
- Cisco SD-Access アクセスセグメンテーションを使用したネットワークセキュリティの強化に関するガイダンスについては、『SD-Accessアクセスセグメンテーション設計ガイド』を参照してください。
- Cisco DNA Center での SDA の展開に関するガイダンスは、『ソフトウェア定義型アクセス導入ガイド』を参照してください。
- Cisco DNA Center と Cisco SD-Access ソリューションの基盤であるデジタル ネットワーク アーキテクチャの詳細と、この革新的なアーキテクチャで他のシスコ製品やソリューション、サードパーティの製品やソリューションが果たす役割については、『Cisco DNA Design Zone』を参照してください。

インターフェイスケーブル接続

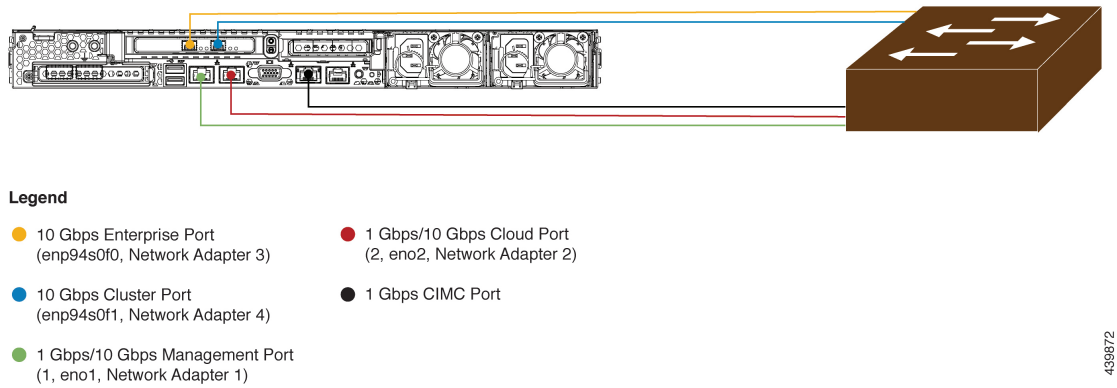
次のタイプのネットワークアクセスを提供するスイッチに、アプライアンスのポートを接続します。Cisco DNA Center の機能に必要なため、最低でも企業およびクラスタのポートインターフェイスを設定する必要があります。

- **（オプション）1Gbps または 10Gbps の管理ポート（1、eno1、ネットワークアダプタ 1）**：このポート（背面パネルに**1**というラベル付き）を使用して Cisco DNA Center のグラフィック ユーザ インターフェイスにアクセスできます。その目的は、ユーザがアプライアンスでソフトウェアを使用できるようにすることです。このポートを、企業管理ネットワークに接続してスイッチにケーブル接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。
- **（オプション）1Gbps または 10Gbps のクラウドポート（2、eno2、ネットワークアダプタ 2）**：このポートは、背面パネルに **2** というラベルが付いており、オプションです。10Gbps のエンタープライズポート（enp94s0f0、ネットワークアダプタ 3）を使用してアプライアンスをインターネット（インターネット プロキシ サーバを含む）に接続できない場合にのみ使用してください。クラウドポートを使用する必要がある場合は、インターネット プロキシ サーバに接続しているスイッチにケーブル接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。
- **（必須）10Gbps エンタープライズポート（enp94s0f0、ネットワークアダプタ 3）**：これはアプライアンス PCIe ライザ 1/スロット 1 の Intel X710-DA2 NIC の左側にあるポートです。その目的は、Cisco DNA Center のネットワークとの通信および管理を有効にすることです。このポートを、エンタープライズネットワークに接続しているスイッチにケーブル接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。
- **（必須）10Gbps クラスタポート（enp94s0f1、ネットワークアダプタ 4）**：これはアプライアンス PCIe ライザ 1/スロット 1 の Intel X710-DA2 NIC の右側にあるポートです。その目的は、クラスタ内のプライマリノードとアドオンノード間の通信を可能にすることです。このポートをクラスタ内の他のノードに接続しているスイッチにケーブル接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

  設定中、Maglev 設定ウィザードは、クラスタリンクオプションをインターフェイスに割り当てるまで続行できません。ポート enp94s0f1 をクラスタリンクとして指定することを推奨します。ただし、クラスタリンクとしてマークされたインターフェイスは、設定が完了した後は変更できないことに注意してください。後でクラスタリンクとしてマークされたインターフェイスを変更する必要がある場合は、再インストールが必要になります。将来的に 3 ノードクラスタへの拡張を可能にするために、IP アドレスを使用してクラスタポートを設定することを推奨します。また、クラスタ リンク インターフェイスがスイッチポートに接続されていて、稼働状態になっていることを確認します。
- **（オプション、ただし強く推奨）1Gbps CIMC ポート**：このポートは、CIMC アウトオブバンド アプライアンス管理インターフェイスとそのグラフィック ユーザ インターフェイスへのブラウザアクセスを提供します。その目的は、アプライアンスとそのハードウェアを管理できるようにすることです。このポートを、企業管理ネットワークに接続してスイッチにケーブル接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

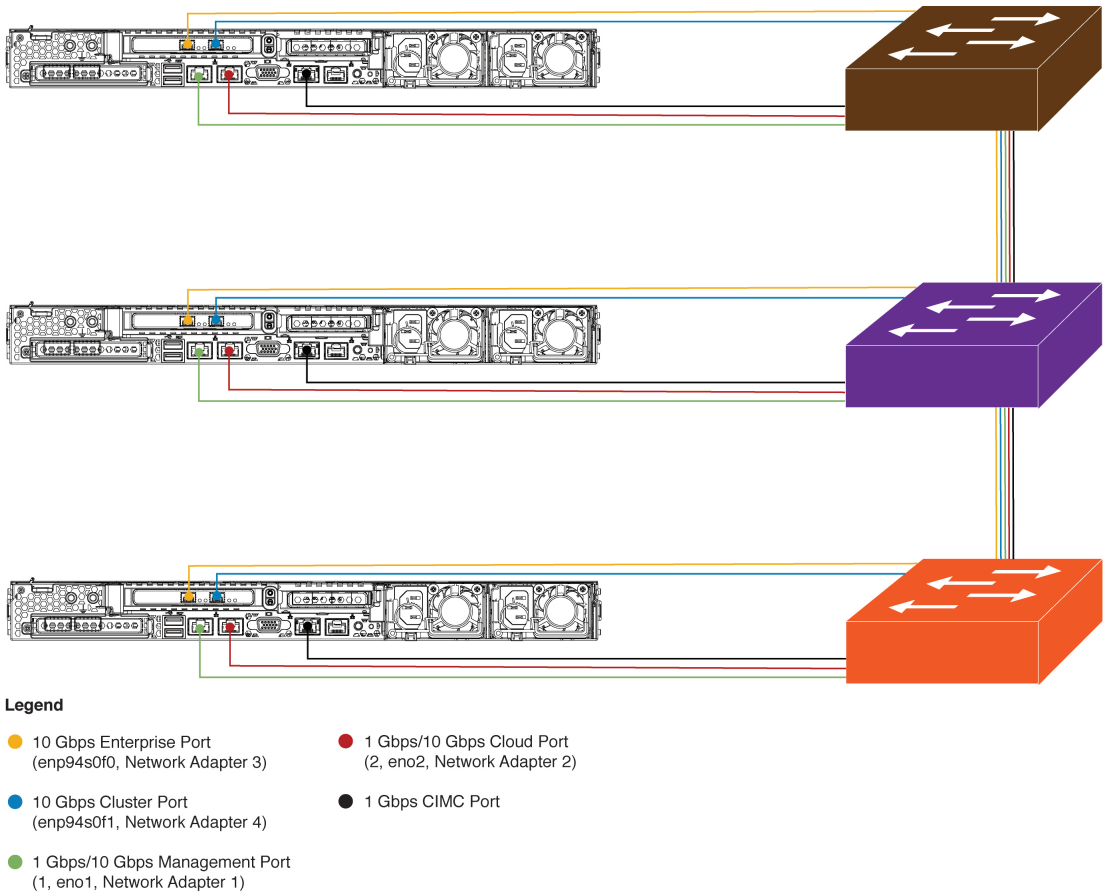
次の図は、単一ノード Cisco DNA Center クラスタの推奨される接続を示しています。

図 *1:* 単一ノードクラスタの推奨される配線



次の図は、3 ノード Cisco DNA Center クラスタの推奨される接続を示しています。3 ノードクラスタ内の各ノードの接続は1つ以外すべて、シングルノードクラスタの場合と同じであり、同じポートを使用します。例外はクラスタポート（enp94s0f1、ネットワークアダプタ 4）であり、これは3ノードクラスタ内の各ホストが他のホストと通信できるようにするために必要です。

図 *2:3* ノードクラスタの推奨される配線



各ポートの詳細については、前面パネルと背面パネルにあるアプライアンスの背面パネルの図と付属の説明を参照してください。

（注） マルチノードクラスタの導入では、すべてのメンバノードを同じサイトの同じネットワーク内にする必要があります。アプライアンスは、複数のネットワークまたはサイト間でのノードの配布をサポートしていません。

10Gbps のエンタープライズポートとクラスタポートを接続する場合は、ポートで次のメディアタイプのみがサポートされていることに注意してください。

- SFP-10G-SR（ショートレンジ、MMF）
- SFP-10G-LR（ロングレンジ、SMF）
- SFP-H10GB-CU1M（Twinax ケーブル、パッシブ、1 m）
- SFP-H10GB-CU3M（Twinax ケーブル、パッシブ、3 m）
- SFP-H10GB-CU5M（Twinax ケーブル、パッシブ、5 m）
- SFP-H10GB-ACU7M（Twinax ケーブル、アクティブ、7 m）

必要な IP アドレスおよびサブネット

設置を開始する前に、使用する予定の各アプライアンスポートに割り当てるのに十分な IP アドレスがネットワークにあることを確認する必要があります。アプライアンスを単一ノードクラスタとして設置するか、3 ノードクラスタのプライマリまたはアドオンノードとして設置するかによって、次のアプライアンスポート（NIC）アドレスが必要になります。

- **エンタープライズ ポート アドレス（Enterprise Port Address）（必須）**：サブネットマスクを持つ 1 つの IP アドレス。
- **クラスタポートアドレス（Cluster Port Address）（必須）**：サブネットマスクを持つ 1 つの IP アドレス。
- **管理ポートアドレス（Management Port Address）（オプション）**：1 つの IP アドレスとサブネットマスク。
- **クラウドポートアドレス（Cloud Port Address）（オプション）**：サブネットマスクを持つ 1 つの IP アドレス。これはオプションのポートであり、エンタープライズポートを使用してクラウドに接続できない場合にのみ使用されます。この目的で使用する必要がある場合を除き、クラウドポートの IP アドレスは必要ありません。
- **CIMCポートアドレス（CIMC Port Address）（オプション、ただし強く推奨）**：サブネットマスクを持つ 1 つの IP アドレス。

（注） これらの要件で要求されるすべての IP アドレスは、有効な IPv4 ネットマスクを持つ有効な IPv4 アドレスである必要があります。アドレスと対応するサブネットが重複していないことを確認します。重複している場合、サービスの通信の問題が発生する可能性があります。

また、次の追加の IP アドレスと専用 IP サブネットが必要になります。これは、アプライアンスの設定時に入力が求められ、適用されます。

1. **クラスタ仮想 IP アドレス（Cluster Virtual IP Addresses）**：クラスタごとに設定されたネットワークインターフェイスごとに 1 つの仮想 IP（VIP）アドレス。この要件は3 ノードクラスタと、将来 3 ノードクラスタに変換される可能性のある単一ノードクラスタに適用されます。設定するネットワークインターフェイスごとに VIP を指定する必要があります。各 VIP は、対応する設定済みインターフェイスの IP アドレスと同じサブネットからのものである必要があります。各アプライアンスには、エンタープライズ、クラスタ、管理、およびクラウドの 4 つのインターフェイスがあります。Cisco DNA Center の機能に必要なため、最低でも企業およびクラスタのポートインターフェイスを設定する必要があります。サブネットマスクと 1 つ以上の関連ゲートウェイまたはスタティックルートとともに IP をインターフェイスに指定すると、そのインターフェイスは設定されていると見なされます。設定時にインターフェイスを完全にスキップすると、そのインターフェイスは設定されていないと見なされます。

   次の点に注意してください。

   - 単一ノード設定で、今後 3 ノードクラスタに変換する予定がない場合は、仮想 IP アドレスを指定する必要はありません。ただし、これを行う場合は、設定されているすべてのネットワーク インターフェイスに仮想 IP アドレスを指定する必要があります（3 ノードクラスタの場合と同様）。
   - 単一ノードクラスタのクラスタ内リンクがダウンすると、管理インターフェイスとエンタープライズ インターフェイスに関連付けられている仮想 IP アドレスもダウンします。このような状況が発生すると、Cisco DNA Center はクラスタ内リンクが復元されるまで使用できなくなります（SWIM と ISE の統合は動作しなくなり、NDP コレクタから情報を収集できないため、アシュアランスデータは表示されません）。

2. **デフォルトゲートウェイ IP アドレス（Default Gateway IP Address）**：ネットワークの優先デフォルトゲートウェイの IP アドレス。他のルートがトラフィックに一致しない場合、トラフィックはこの IP アドレスを経由してルーティングされます。通常は、インターネットにアクセスするネットワーク設定内のインターフェイスにデフォルトゲートウェイを割り当てます。Cisco DNA Center の導入時に留意すべきセキュリティ上の考慮事項については、『Cisco DNA Center Security Best Practices Guide』を参照してください。

3. [DNS Server IP Addresses]：1 つ以上のネットワークの優先 DNS サーバの IP アドレス。設定時に、複数の DNS サーバの IP アドレスとネットマスクを、スペースで区切ったリストとして入力することによってそれらを指定できます。

4. **（オプション）スタティックルートアドレス（Static Route Addresses）**：1 つ以上のスタティックルートの IP アドレス、サブネットマスク、およびゲートウェイ。設定時に、複数

のスタティックルートの IP アドレス、ネットマスク、およびゲートウェイを、スペースで区切ったリストとして入力することによってそれらを指定できます。

アプライアンスの任意のインターフェイスに対して 1 つ以上のスタティックルートを設定できます。デフォルトゲートウェイ以外の特定の方向でトラフィックをルーティングする場合は、スタティックルートを指定する必要があります。スタティックルートを持つ各インターフェイスは、IP route コマンドテーブルでトラフィックがルーティングされる「デバイス」として設定されます。このため、トラフィックが送信されるインターフェイスとスタティックルートの方向を一致させることが重要です。

スタティックルートは、スイッチやルータで使用されるようなネットワークデバイスのルーティングテーブルでは推奨されません。この場合はダイナミック ルーティング プロトコルの方が適しています。ただし、他の方法では到達できないネットワークの特定の部分にアプライアンスがアクセスできるようにするには、必要に応じてそれらを追加する必要があります。

5. [NTP Server IP Addresses]：DNS 解決可能なホスト名、または 1 つ以上の Network Time Protocol（NTP）サーバの IP アドレス。

   設定時に、複数の NTP サーバの IP やマスクまたはホスト名をスペースで区切ったリストとして入力することによって、それらを指定できます。実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定することを推奨します。

   これらのサーバは、事前にハードウェアを同期するときに指定し、クラスタ内の各アプライアンスでソフトウェアを設定する際に再度指定します。時刻の同期は、マルチホストクラスタ全体でのデータの精度と処理の調整にとって重要です。アプライアンスを実稼働環境に展開する前に、アプライアンスのシステムクロックの時刻が現在の時刻であること、および指定した Network Time Protocol（NTP）サーバが正確な時刻を維持していることを確認してください。アプライアンスを Cisco Identity Services Engine（ISE）と統合する予定の場合は、ISE がアプライアンスと同じ NTP サーバと同期していることも確認する必要があります。

6. [サービスサブネット（Services Subnet）]：アシュアランス、インベントリ収集などの内部アプリケーションサービス間の通信用 IP を管理および取得する際にアプライアンスが使用する 1 つの専用 IP サブネットを識別します。専用 IPv4 サービスサブネットは、Cisco DNA Center の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりすることはできません。サブネットの最小サイズは 21 ビットです。IPv4 サービスサブネットは、次のアドレス範囲をサポートするプライベートネットワークの IETF RFC 1918 および RFC 6598 仕様に準拠している必要があります。

   - 10.0.0.0/8
   - 172.16.0.0/12
   - 192.168.0.0/16
   - 100.64.0.0/10

   詳細については、RFC 1918 では『Address Allocation For Private Internets』を、RFC 6598 では『 IANA-Reserved IPv4 Prefix For Shared Address Space 』を参照してください。

（注）

- 有効なCIDRサブネットが指定されていることを確認します。そうでない場合、172.17.1.0/20 および 172.17.61.0/20 サブネットに誤ったビットが表示されます。
- Cisco DNA Center アプライアンスの設定が完了したら、最初にアプライアンスを再イメージ化せずに別のサブネットを割り当てることはできません（詳細については、「アプライアンスの設定」章の「アプライアンスの再イメージ化」のトピックを参照してください）。

7. [クラスタサービスサブネット（Cluster Services Subnet）]：データベースアクセス、メッセージバスなどのインフラストラクチャ サービス間の通信用 IP を管理および取得する際にアプライアンスが使用する 1 つの専用 IP サブネットを識別します。専用 IPv4 クラスタサービスサブネットは、Cisco DNA Centerの内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりすることはできません。サブネットの最小サイズは 21 ビットです。IPv4 クラスタサービスサブネットは、次のアドレス範囲をサポートするプライベートネットワークの IETF RFC 1918 および RFC 6598 仕様に準拠している必要があります。
   - 10.0.0.0/8
   - 172.16.0.0/12
   - 192.168.0.0/16
   - 100.64.0.0/10

   詳細については、RFC 1918 では『Address Allocation For Private Internets』を、RFC 6598 では『 IANA-Reserved IPv4 Prefix For Shared Address Space 』を参照してください。

   サービスサブネットとして 10.10.10.0/21 を指定する場合は、これら 2 つのサブネットは重複しないため、10.0.8.0/21 のクラスタサービスサブネットを指定することもできます。また、設定ウィザードによって、これらのサブネット間の重複（存在する場合）が検出され、重複を修正するように求められることにも注意してください。

（注）

- 有効なCIDRサブネットが指定されていることを確認します。そうでない場合、172.17.1.0/20 および 172.17.61.0/20 サブネットに誤ったビットが表示されます。
- Cisco DNA Center アプライアンスの設定が完了したら、最初にアプライアンスを再イメージ化せずに別のサブネットを割り当てることはできません（詳細については、「アプライアンスの設定」章の「アプライアンスの再イメージ化」のトピックを参照してください）。

2つのサービスとクラスタサービスのサブネットで推奨される合計IPアドレス空間には、4096 のアドレスが含まれており、それぞれ 2048 のアドレスの 2/21 サブネットに分割されています。2/21 サブネットを重複させることはできません。Cisco DNA Center の内部サービスは、専用のIPアドレスセットの動作に必要です（Cisco DNA Centerマイクロサービス アーキテクチャ

の要件）。この要件に対応するには、Cisco DNA Center システムごとに 2 つの専用サブネットを割り当てる必要があります。

アプライアンスがこのようなアドレス空間を必要とする理由の 1 つは、システムパフォーマンスを維持するためです。東西（ノード間）通信には内部ルーティングおよびトンネリングテクノロジーが使用されているため、重複するアドレス空間を使用すると、アプライアンスが仮想ルーティングを実行し、内部的に FIB を転送するように強制されることがあります。これにより、1 つのサービスから別のサービスに送信されるパケットに対して複数の encap/decap が発生し、高いレイヤでのカスケードの影響により、非常に低いレベルの高い内部遅延が発生します。

もう 1 つの理由は Cisco DNA Center Kubernetes ベースのサービスコンテナ化アーキテクチャです。各アプライアンスは、Kubernetes K8 ノードごとにこの空間の IP アドレスを使用します。複数のノードが 1 つのサービスを構成できます。現在、Cisco DNA Centerは、複数の IP アドレスを必要とするサービスを 100 以上サポートしており、新しい機能と対応するサービスが常に追加されています。最初は意図的に大きなアドレス空間を確保するように要求されます。これは、IP が不足することなく、また単にシステムをアップグレードするだけのために連続するアドレス空間の再割り当てをお客様に求めることなく、シスコが新しいサービスや機能を追加できるようにするためです。

これらのサブネットでサポートされているサービスは、レイヤ 3 でも有効になっています。クラスタサービススペースは、特に、アプリケーションサービスとインフラストラクチャ サービスの間でデータを伝送し、頻繁に使用されます。

RFC 1918 および RFC 6598 の要件は、クラウドからパッケージとアップデートをダウンロードするための Cisco DNA Center の要件によるものです。選択した IP 範囲が RFC 1918 および RFC 6598 に準拠していない場合、すぐにパブリック IP の重複の問題につながる可能性があります。

インターフェイス名とウィザードの設定順序

インターフェイス名と、これらのインターフェイスを Maglev 設定ウィザードで設定する順序は、次の表に示すように、Cisco DNA Center アプライアンスの第 1 世代と第 2 世代とで異なります。お使いのアプライアンスが第 1 世代と第 2 世代のどちらかを判断するには、次のとおりシスコ製品番号を参照してください。

- 第 1 世代 44 コアアプライアンス：DN1-HW-APL
- 第 2 世代：
  - 44 コアアプライアンス：DN2-HW-APL
  - 44 コア アップグレード アプライアンス：DN2-HW-APL-U
  - 56 コアアプライアンス：DN2-HW-APL-L

表 *2:* インターフェイス名とウィザードの設定順序

機能	Cisco DNA Center アプライアンスの種類	インターフェイス名	Maglev設定ウィザードでの設定順序
管理：管理ネットワークから Cisco DNA Center GUI にアクセスできます。	第 1 世代	enp1s0f0	ネットワークアダプタ #2
	第 2 世代	**eno1**	**ネットワークアダプタ #1**
クラウド：この目的で別のインターフェイスを使用できない場合にインターネットアクセスを提供します。	第 1 世代	enp1s0f1	ネットワークアダプタ #3
	第 2 世代	**eno2**	**ネットワークアダプタ #2**
エンタープライズ：アプライアンスをエンタープライズ ネットワークにリンクします。	第 1 世代	enp9s0	ネットワークアダプタ #4
	第 2 世代	**enp94s0f0**	**ネットワークアダプタ #3**
クラスタ：アプライアンスをクラスタノードにリンクします。	第 1 世代	enp10s0	ネットワークアダプタ #1
	第 2 世代	**enp94s0f1**	**ネットワークアダプタ #4**

必要なインターネット URL と完全修飾ドメイン名

アプライアンスでは、次の URL と完全修飾ドメイン名（FQDN）の表へのセキュアなアクセスが必要です。

この表では、各 URL と FQDN を使用する機能について説明します。IP トラフィックがアプライアンスとこれらのリソースとの間を移動できるように、ネットワーク ファイアウォールまたはプロキシサーバのいずれかを設定する必要があります。リストされている URL と FQDN にこのアクセスを提供できない場合は、関連付けられている機能が損なわれるか、または動作不能になります。

インターネットへのプロキシアクセスの要件の詳細については、「インターネットへのアクセスを保護」を参照してください。

表 3 : 必要な URL と FQDN アクセス

目的	...Cisco DNA Center がアクセスする必要がある URL と FQDN
システムとアプリケーション パッケージ ソフトウェアにアップデートをダウンロードし、製品チームにユーザからのフィードバックを送信します。	推奨：*.ciscoconnectdna.com:443[1] ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 • https://www.ciscoconnectdna.com • https://cdn.ciscoconnectdna.com • https://registry.ciscoconnectdna.com • https://registry-cdn.ciscoconnectdna.com
Cisco DNA Center パッケージの更新	https://*.ciscoconnectdna.com/*
スマートアカウントおよび SWIM ソフトウェアのダウンロード	https://apx.cisco.com https://cloudsso.cisco.com/as/token.oauth2 https://*.cisco.com/*
ユーザフィードバック	https://dnacenter.uservoice.com
Cisco Meraki との統合	推奨：*.meraki.com:443 ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 • dashboard.meraki.com:443 • api.meraki.com:443 • n63.meraki.com:443

目的	...Cisco DNA Center がアクセスする必要がある URL と FQDN
Cisco.com とシスコ スマートライセンスとの統合	*.cisco.com:443 ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 • software.cisco.com • cloudsso.cisco.com • cloudsso1.cisco.com • cloudsso2.cisco.com • apiconsole.cisco.com • api.cisco.com • apx.cisco.com • sso.cisco.com • apmx-prod1-vip.cisco.com • apmx-prod2-vip.cisco.com
サイトとロケーションマップで正確な情報をレンダリング	• www.mapbox.com • *. tiles.mapbox.com/*: 443 プロキシの場合、宛先は *.tiles.mapbox.com/* です。

[1] シスコは ciscoconnectdna.com とそのサブドメインを所有し、維持しています。Cisco Connect DNA インフラストラクチャは、シスコのセキュリティおよび信頼に関するガイドラインを満たし、継続的なセキュリティテストを実施しています。このインフラストラクチャは堅牢であり、組み込みのロードバランシング機能と自動化機能を備えています。24 時間 365 日の可用性を確保するために、クラウド運用チームが監視と保守を行います。

インターネットへのアクセスを保護

デフォルトでは、アプライアンスは、インターネット経由で Cisco.com およびその他の URL にアクセスして、ソフトウェアアップデート、ライセンス、およびデバイスソフトウェアをダウンロードしたり、最新のマップ情報、ユーザフィードバックなどを提供したりするように設定されています。

これらの目的でインターネット接続を提供することは必須要件です。

HTTPS プロキシサーバを使用することは、リモート URL に安全にアクセスするための信頼性の高い方法です。必要なインターネット URL と完全修飾ドメイン名 に記載されている URL に必要とするアクセスをアプライアンスに提供するには、HTTPS プロキシサーバを使用することをお勧めします。設置時に、この目的で使用するプロキシサーバの URL とポート番号を、

プロキシのログインクレデンシャルとともに入力するように求められます（プロキシが必要な場合）。

このリリースでは、アプライアンスはHTTPを介したプロキシサーバとの通信のみをサポートしています。HTTPS プロキシサーバは、ネットワーク内の任意の場所に配置できます。プロキシサーバは HTTPS を使用してインターネットと通信できますが、アプライアンスは HTTP 経由でプロキシサーバと通信します。このような理由から、設定時にプロキシを設定する場合は、必ずプロキシの HTTP ポートを指定する必要があります。

何らかの理由で設定後にプロキシ設定を変更する必要がある場合は、GUIインターフェイスを使用して行うことができます。

必要なネットワークポート

次の表に、アプライアンスが使用する既知のネットワークサービスポートを示します。これらのポートが、ファイアウォール設定またはプロキシゲートウェイのどちらで開くかを問わず、アプライアンスとの間で送受信されるトラフィックフローに対して開いていることを確認する必要があります。

SDAインフラストラクチャを採用するネットワークにアプライアンスを導入する場合は、追加のポート、プロトコル、およびトラフィックタイプに対応している必要があります。詳細については、「必要な SD アクセス ポートおよびプロトコル」を参照してください。

（注） Cisco DNA Center の導入時に留意すべきセキュリティ上の考慮事項については、『Cisco Digital Network Architecture Center Security Best Practices Guide』を参照してください。

表 *4:* ポート：着信トラフィック

ポート番号	許可されるトラフィック	プロトコル（TCP または UDP）
80	HTTP	TCP
111	NFS（アシュアランスのバックアップに使用）	TCP および UDP
123	NTP	UDP
162	SNMP	UDP
443	HTTPS	TCP
2049	NFS（アシュアランスのバックアップに使用）	TCP および UDP
2222	SSH	TCP

ポート番号	許可されるトラフィック	プロトコル（TCPまたはUDP）
20048	NFS（アシュアランスのバックアップに使用）	TCP および UDP
32767	NFS（アシュアランスのバックアップに使用）	TCP および UDP

表 *5:* ポート：発信トラフィック

ポート番号	許可されるトラフィック	プロトコル（TCPまたはUDP）
22	SSH（ネットワークデバイスと Cisco ISE へ）	TCP
23	Telnet（ネットワーク デバイスへ）	TCP
53	DNS	UDP
80	ポート 80 は出力プロキシ設定に使用できます。 さらに、プロキシが設定ウィザードによって設定されている場合（プロキシがすでにネットワークに使用されている場合）、8080 などの他の一般的なポートも使用できます。 シスコでサポートされている証明書およびトラストプールにアクセスするには、アプライアンスから次の URL にあるシスコのアドレスへの発信 IP トラフィックを許可するようにネットワークを設定できます。 https://www.cisco.com/security/pki/	TCP
123	NTP	UDP
161	SNMP エージェント	UDP
443	HTTPS	[TCP]
5222	PxGrid の ISE XMP	TCP

ポート番号	許可されるトラフィック	プロトコル（TCP または UDP）
9060	ISE ERS の API トラフィック	TCP

次の表に、アプライアンスへの着信 IP トラフィックを許可するポートを示します。

表 *6 :* ポート：*IP* トラフィック

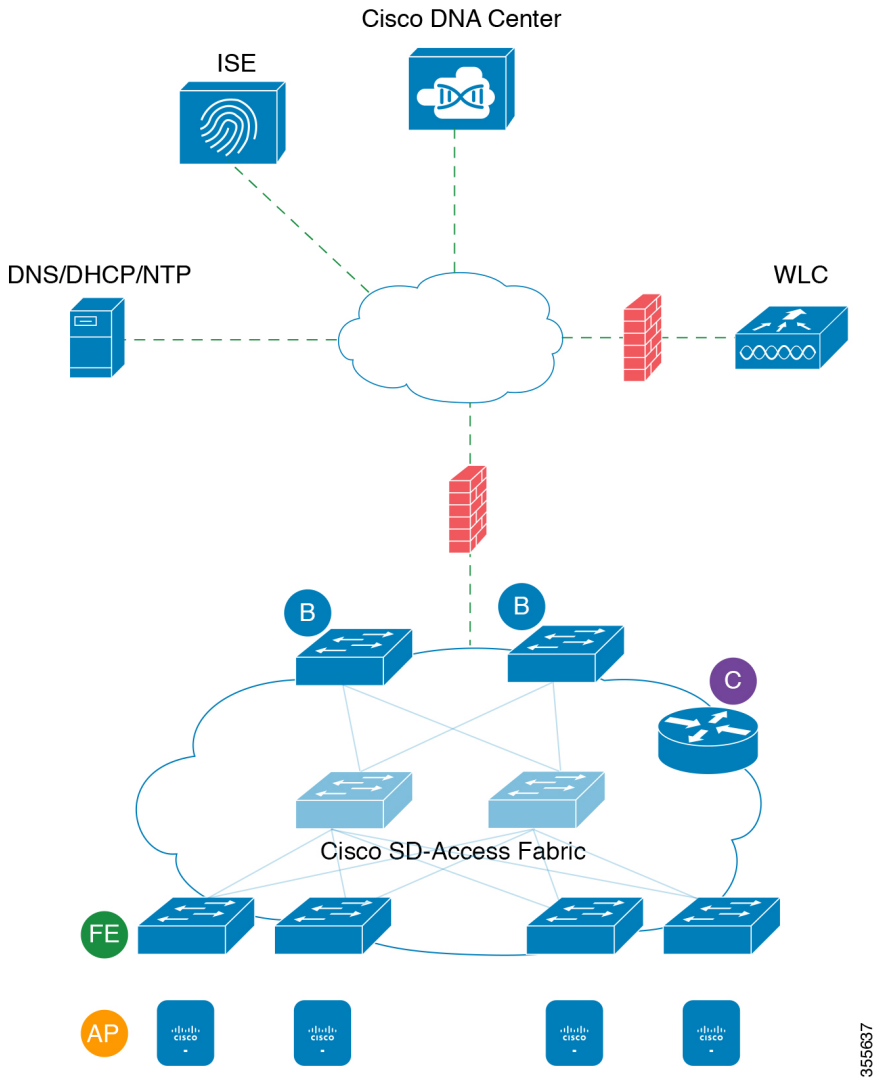
プロトコル（TCP または UDP）	ポート番号	トラフィックのタイプ
TCP	22	SSH
TCP	2222	SSH
TCP	80	HTTP
TCP	443	HTTPS
UDP	67	bootps
UDP	123	NTP
UDP	162	SNMP

さらに、アプライアンスから次の URL にあるシスコのアドレスへの発信 IP トラフィックを許可するようにネットワークを設定できます。https://www.cisco.com/security/pki/アプライアンスからシスコがサポートする証明書およびトラストプールにアクセスするには、上述の URL に記載されている IP アドレスを使用します。

必要な SD アクセス ポートおよびプロトコル

このトピックでは、次の図に示すように、一般的なSDAファブリック導入にネイティブなポート、プロトコル、およびトラフィックのタイプについて詳しく説明します。

図 *3: SDA* ファブリック インフラストラクチャ



ネットワークに SDA を実装している場合は、次の表の情報を使用して、ネットワーク管理を自動化するために必要なアクセスを Cisco DNA Center に提供しながら、SDA インフラストラクチャを適切に保護するファイアウォールとセキュリティポリシーを計画します。

表 *7: Cisco DNA Center* トラフィック

送信元ポート[2]	送信元	宛先ポート	接続先	説明
任意	Cisco DNA Center	UDP 53	DNS Server	Cisco DNA Center から DNS サーバの間で使用

任意	Cisco DNA Center	TCP 22	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で SSH に使用
任意	Cisco DNA Center	TCP 23	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で Telnet に使用
任意	Cisco DNA Center	UDP 161	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で SNMP デバイス検出に使用
ICMP	Cisco DNA Center	ICMP	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で SNMP デバイス検出に使用
任意	Cisco DNA Center	TCP 443	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間でソフトウェアアップグレードに使用（プロキシがない場合はインターネットへの間でも使用）
任意	Cisco DNA Center	TCP 80	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間で PnP に使用（プロキシがない場合はインターネットへの間でも使用）
任意	Cisco DNA Center	TCP 830	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間で Netconf に使用（SDA 組み込みワイヤレス）
UDP 123	Cisco DNA Center	UDP 123	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間で LAN 自動化中の初期に使用
任意	Cisco DNA Center	UDP 123	NTP Server	Cisco DNA Center から NTP サーバの間で使用
任意	Cisco DNA Center	TCP 22、UDP 161	WLC	Cisco DNA Center から WLC へ
ICMP	Cisco DNA Center	ICMP	WLC	Cisco DNA Center から WLC へ
任意	Cisco DNA Center	TCP 80、TCP 443	AP	Cisco DNA Center からセンサー、アクティブセンサー（Cisco Aironet 1800S）の AP の間で使用

任意	Cisco DNA Center	TCP 32626	AP	Cisco DNA Center から AP へ（gRPC 用）

[2] のクラスタ、PKI、SFTP サーバ、プロキシポートのトラフィックは、この表には含まれていません。

表 *8:* インターネット接続トラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
任意	Cisco DNA Center	TCP 443	registry.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
任意	Cisco DNA Center	TCP 443	www.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
任意	Cisco DNA Center	TCP 443	registry-cdn.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
任意	Cisco DNA Center	TCP 443	cdn.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
任意	Cisco DNA Center	TCP 443	software.cisco.com	デバイスソフトウェアのダウンロード
任意	Cisco DNA Center	TCP 443	cloudsso.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
任意	Cisco DNA Center	TCP 443	cloudsso1.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
任意	Cisco DNA Center	TCP 443	cloudsso2.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
任意	Cisco DNA Center	TCP 443	apiconsole.cisco.com	CSSM スマートライセンス API
任意	Cisco DNA Center	TCP 443	sso.cisco.com	CCO とスマートライセンス
任意	Cisco DNA Center	TCP 443	api.cisco.com	CCO とスマートライセンス

任意	Cisco DNA Center	TCP 443	apx.cisco.com	CCO とスマートライセンス
任意	Cisco DNA Center	TCP 443	dashboard.meraki.com	Meraki の統合
任意	Cisco DNA Center	TCP 443	api.meraki.com	Meraki の統合
任意	Cisco DNA Center	TCP 443	n63.meraki.com	Meraki の統合
任意	Cisco DNA Center	TCP 443	dnacenter.uservoice.com	ユーザフィードバックの送信
任意	Cisco DNA Center Admin Client	TCP 443	*.tiles.mapbox.com	ブラウザでのマップのレンダリング（プロキシ経由のアクセスの場合、宛先は *.tiles.mapbox.com/*）
任意	Cisco DNA Center	TCP 443	www.mapbox.com	マップと WLC の国番号の識別

表 *9 : SDA* ファブリック アンダーレイ トラフィック

送信元ポート[3]	送信元	宛先ポート	接続先	説明
UDP 68	ファブリックアンダーレイ	UDP 67	DHCP サーバ	ファブリックスイッチおよびルータと DHCP サーバの間で、ファブリックエッジノードによって開始される DHCP リレーパケット用に使用されます。
任意	ファブリックアンダーレイ	TCP 80	Cisco DNA Center	ファブリックスイッチおよびルータのループバック IP と Cisco DNA Center の間で PnP 用に使用
任意	ファブリックアンダーレイ	TCP 443	Cisco DNA Center	ファブリックスイッチ、ルータループバック IP から Cisco DNA Center の間でイメージのアップグレードに使用
任意	ファブリックアンダーレイ	UDP 162	Cisco DNA Center	ファブリックスイッチ、ルータループバック IP から Cisco DNA Center の間で SNMP トラップに使用

任意	ファブリックアンダーレイ	UDP 514	Cisco DNA Center	ファブリックスイッチおよびルータと Cisco DNA Center の間でアシュアランス用に使用
任意	ファブリックアンダーレイ	UDP 6007	Cisco DNA Center	ファブリックルータから Cisco DNA Center の間で NetFlow に使用
任意	ファブリックアンダーレイ	UDP 123	Cisco DNA Center	ファブリックスイッチから Cisco DNA Center の間で LAN 自動化時に使用
ICMP	ファブリックアンダーレイ	ICMP	Cisco DNA Center	ファブリックスイッチ、ルータループバックから Cisco DNA Center の間で SNMP デバイス検出に使用
UDP 161	ファブリックアンダーレイ	任意	Cisco DNA Center	ファブリックスイッチおよびルータのループバックと Cisco DNA Center の間で SNMP デバイス検出のために使用
任意	ファブリックアンダーレイ	UDP 53	DNS Server	ファブリックスイッチ、ルータから DNS サーバの間で名前解決に使用
TCP および UDP 4342	ファブリックアンダーレイ	TCP および UDP 4342	ファブリックルータおよびスイッチ	LISP カプセル化制御メッセージ
TCP および UDP 4342	ファブリックアンダーレイ	任意	ファブリックルータおよびスイッチ	LISP コントロールプレーン通信
任意	ファブリックアンダーレイ	UDP 4789	ファブリックルータおよびスイッチ	ファブリックカプセル化データパケット（VXLAN-GPO）
任意	ファブリックアンダーレイ	UDP 1645/1646/1812/1813	ISE	ファブリックスイッチおよびルータのループバック IP と ISE の間で RADIUS 用に使用
ICMP	ファブリックアンダーレイ	ICMP	ISE	ファブリックスイッチ、ルータから ISE の間でトラブルシューティングに使用
UDP 1700/3799	ファブリックアンダーレイ	任意	ISE	ファブリックスイッチと ISE の間で CoA 用に使用

任意	ファブリックアンダーレイ	UDP 123	NTP Server	ファブリックスイッチおよびルータのループバック IP と NTP サーバの間で使用
任意	control-plane	UDP および TCP 4342/4343	WLC	コントロールプレーンのループバック IP と WLC の間でファブリック対応ワイヤレス用に使用

[3] ボーダー ルーティング プロトコル、SPAN、プロファイリング、およびテレメトリ トラフィックは、この表には含まれていません。

表 *10*：ワイヤレス *LAN* コントローラ（*WLC*）トラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 5246/5247/5248	WLC	任意	AP IP プール	WLC と AP サブネットの間で CAPWAP 用に使用
ICMP	WLC	ICMP	AP IP プール	WLC と Ping を許可する AP の間でトラブルシューティングのために使用
任意	WLC	UDP 69/5246/5247 TCP 22	AP IP プール	WLC と AP サブネットの間で CAPWAP 用に使用
任意	WLC	UDP および TCP 4342/4343	コントロールプレーン	WLC とコントロールプレーンループバック IP の間で使用
任意	WLC	TCP 32222	Cisco DNA Center	WLC と Cisco DNA Center の間でデバイス検出のために使用
UDP 161	WLC	任意	Cisco DNA Center	WLC と Cisco DNA Center の間で SNMP 用に使用
任意	WLC	UDP 162	Cisco DNA Center	WLC と Cisco DNA Center の間で SNMP トラップ用に使用
任意	WLC	TCP 16113	MSE および Spectrum Expert	WLC と MSE および Spectrum Expert の間で NMSP 用に使用
ICMP	WLC	ICMP	Cisco DNA Center	WLCから、トラブルシューティングに向けた Ping の許可に使用
任意	HA サーバ	TCP 1315	Cisco DNA Center	データベースサーバ HA（QoS）
任意	HA サーバ	TCP 1316 ～ 1320	Cisco DNA Center	HA データベースポート

任意	HA Web サーバ	TCP 8082	Cisco DNA Center	HA Web サーバのヘルスモニタポート
任意	WLC および各種 Syslog サーバ	UDP 514	WLC	Syslog（オプション）
任意	WLC	UDP 53	DNS Server	WLC と DNS サーバの間で使用
任意	WLC	TCP 443	ISE	WLC と ISE の間でゲスト SSID Web 認証のために使用
任意	WLC	UDP 1645、1812	ISE	WLC と ISE の間で RADIUS 認証のために使用
任意	WLC	UDP 1646、1813	ISE	WLC と ISE の間で RADIUS アカウンティングのために使用
任意	WLC	UDP 1700、3799	ISE	WLC と ISE の間で RADIUS CoA 用に使用
ICMP	WLC	ICMP	ISE	WLC と ISE ICMP の間でトラブルシューティングのために使用
任意	WLC	UDP 123	NTP サーバ	WLC と NTP サーバの間で使用

表 *11 :* ファブリック対応ワイヤレスアクセスポイント（*AP*）の *IP* プールトラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 68	AP IP プール	UDP 67	DHCP サーバ	AP IP プールと DHCP サーバの間で使用
ICMP	AP IP プール	ICMP	DHCP サーバ	AP IP プールと ICMP の間でトラブルシューティングのために使用
任意	AP IP プール	514	各種	Syslog：宛先設定可能。デフォルトは 255.255.255.255
任意	AP IP プール	UDP 69/5246/5247/5248	WLC	AP IP プールと WLC の間で CAPWAP 用に使用
ICMP	AP IP プール	ICMP	WLC	AP IP プールから WLC に送信。トラブルシューティングのために Ping を許可

表 *12 : Identity Services Engine*（*ISE*）トラフィック

送信元ポート[4]	送信元	宛先ポート	接続先	説明

任意	ISE	TCP 64999	Border	ISE とボーダーノードの間で SXP 用に使用
任意	ISE	UDP 514	Cisco DNA Center	ISE から Syslog サーバ（Cisco DNA Center）の間で使用
UDP 1645/1646/1812/1813	ISE	任意	ファブリックアンダーレイ	ISE からファブリックスイッチ、ルータの間で RADIUS と認証用に使用
任意	ISE	UDP 1700/3799	ファブリックアンダーレイ	ISE とファブリックスイッチおよびルータのループバック IP の間で気付アドレス用に使用
ICMP	ISE	ICMP	ファブリックアンダーレイ	ISE からファブリックスイッチの間でトラブルシューティングに使用
任意	ISE	UDP 123	NTP Server	ISE と NTP サーバの間で使用
UDP 1812/1645/1813/1646	ISE	任意	WLC	ISE と WLC の間で RADIUS 用に使用
ICMP	ISE	ICMP	WLC	ISE と WLC の間でトラブルシューティングのために使用

[4] 注：高可用性およびプロファイリング トラフィックは、この表には含まれていません。

表 *13 : DHCP* サーバトラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 67	DHCP サーバ	UDP 68	AP IP プール	DHCP サーバからファブリック AP の間で使用
ICMP	DHCP サーバ	ICMP	AP IP プール	トラブルシューティング用の ICMP：ファブリックから DHCP の間で使用
UDP 67	DHCP サーバ	UDP 68	ファブリックアンダーレイ	DHCP からファブリックスイッチ、ルータの間で使用
ICMP	DHCP サーバ	ICMP	ファブリックアンダーレイ	トラブルシューティング用の ICMP：ファブリックから DHCP の間で使用
UDP 67	DHCP サーバ	UDP 68	ユーザ IP プール	DHCP サーバからファブリックスイッチ、ルータの間で使用
ICMP	DHCP サーバ	ICMP	ユーザ IP プール	トラブルシューティング用の ICMP：ユーザと DHCP の間で使用

表 *14 : NTP* サーバトラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 123	NTP Server	任意	ISE	NTP サーバから ISE の間で使用
UDP 123	NTP Server	任意	Cisco DNA Center	NTP サーバから Cisco DNA Center
UDP 123	NTP Server	任意	ファブリックアンダーレイ	NTP サーバとファブリックスイッチおよびルータのループバックの間で使用
UDP 123	NTP Server	任意	WLC	NTP サーバと WLC の間で使用

表 *15 : DNS* サーバトラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 53	DNS Server	任意	ファブリックアンダーレイ	DNS サーバからファブリックスイッチの間で使用
UDP 53	DNS Server	任意	WLC	DNS サーバと WLC の間で使用

必須の設定情報

アプライアンスの設定中、必要な IP アドレスおよびサブネットに加えて、次の情報を入力するように求められます。

1. **Linux ユーザ名（Linux User Name）**：これは **maglev** です。このユーザ名はプライマリノードとアドオンノードの両方を含む、クラスタ内のすべてのアプライアンスで共通していて、変更できません。

2. **Linuxパスワード（Linux Password）**：Linux ユーザ名 **maglev** のパスワードを指定します。このパスワードは、Linux コマンドラインを使用して各アプライアンスへのセキュアなアクセスを保証します。選択した場合は、クラスタ内の各アプライアンスの Linux ユーザ名 **maglev** ごとに異なる Linux パスワードを割り当てることができます。

   デフォルト値はないため、ユーザがLinuxパスワードを作成する必要があります。パスワードは次の要件を満たしている必要があります。

   - 長さが 8 文字以上である。
   - タブまたは改行を含まない。
   - 次の中から少なくとも 3 つのカテゴリの文字を含む。

- 大文字のアルファベット
- 小文字のアルファベット
- 数字
- 特殊文字（! や # など）

Linux パスワードは暗号化され、Cisco DNA Center データベースにハッシュされます。マルチノードクラスタを展開している場合は、各アドオンノードにプライマリノードの Linux パスワードを入力するように求められます。

3. [パスワード生成シード（Password Generation Seed）]（オプション）：Linux パスワードを作成する代わりに、シードフレーズを入力し、[パスワードの生成（Generate Password）] を押すことができます。Maglev 設定ウィザードは、そのシードフレーズを使用してランダムかつ安全なパスワードを生成します。[自動生成パスワード（Auto Generated Password）] フィールドを使用して、生成されたパスワードをさらに編集できます。

4. **管理者パスフレーズ（Administrator Passphrase）**：クラスタ内の Cisco DNA Center への Web アクセスに使用されるパスワードを指定します。これはスーパーユーザ権限を持つ管理者のアカウント **admin** のパスワードであり、初めて Cisco DNA Center にログインするときに使用します（「初回ログイン」を参照）。安全であることを確認するため、初回ログイン時にこのパスワードを変更するように求められます。

   このパスワードにはデフォルトがないため、作成する必要があります。管理者のパスフレーズは、上記で説明した Linux パスワードと同じ要件を満たす必要があります。

5. [CIMCユーザパスワード（CIMC User Password）]：CIMC グラフィック ユーザ インターフェイスへのアクセスに使用するパスワードを指定します。工場出荷時のデフォルトは *password* ですが、Web ブラウザ経由でアクセスするために CIMC を初回セットアップするときに変更するように求められます（「CIMC へのブラウザアクセスの有効化」を参照）。

   CIMC ユーザパスワードは、上記で説明した Linux パスワードと同じ要件を満たす必要があります。工場出荷時の初期状態にリセットした場合にのみ、*password* に戻すことができます。

6. **プライマリノード IP アドレス（Primary Node IP Address）**：クラスタにアドオンノードをインストールする場合にのみ必要です。これは、プライマリノード上のクラスタポートの IP アドレスです（「インターフェイスケーブル接続」を参照）。

必要な初期設定情報

アプライアンスの設定が完了したら、Cisco DNA Center に初回ログインし、基本的なセットアップタスクを完了します。この初回設定時には、次の情報が必要になります。

1. **スーパーユーザ権限を持つ管理者の新しいパスワード（New Admin Superuser Password）**：Cisco DNA Center 管理者の新しいスーパーユーザパスワードを入力するように求められます。スーパーユーザ権限を持つ管理者のパスワードをリセットすると、運用上のセキュリ

ティが向上します。これは、たとえば、Cisco DNA Center アプライアンスを設置して設定した企業スタッフが Cisco DNA Center のユーザまたは管理者ではない場合に特に重要です。

2. **Cisco.comログイン情報（Cisco.com Credentials）**：ソフトウェアのダウンロードを登録し、電子メールでシステム通信を受信するために組織が使用する Cisco.com ユーザ ID とパスワード。

3. **シスコ スマートアカウントのクレデンシャル（Cisco Smart Account Credentials）**：組織がデバイスとソフトウェアライセンスの管理に使用する Cisco.com スマートアカウントのユーザ ID とパスワード。

4. **IPアドレスマネージャのURLとクレデンシャル（IP Address Manager URL and Credentials）**：Cisco DNA Center で使用する予定のサードパーティ製 IP アドレスマネージャ（IPAM）サーバのホスト名、URL、管理者ユーザ名、管理者パスワード。現在のリリースでは、InfoBlox または Bluecat がサポートされています。

5. **プロキシURL、ポート、クレデンシャル（Proxy URL, Port and Credentials）**：Cisco DNA Center ソフトウェアのアップデートの取得、デバイスライセンスの管理などのダウンロード可能なコンテンツの取得のために Cisco DNA Center で使用するプロキシサーバの URL（ホスト名または IP アドレス）、ポート番号、ユーザ名、ユーザパスワード。

6. **Cisco DNA Centerユーザ（Users）**：作成する新規 Cisco DNA Center ユーザのユーザ名、パスワード、権限の設定。シスコでは、通常の Cisco DNA Center のすべての操作に対して、これらの新しいユーザアカウントのいずれかを常に使用することを推奨しています。Cisco DNA Center の再設定や、スーパーユーザ権限が明示的に必要なその他の操作を除き、管理者スーパーユーザアカウントを使用することは避けてください。

この情報を入力する初回セットアップウィザードを起動して対応する方法の詳細については、「初回ログイン」を参照してください。

また残りの設定タスクを完了するために次の情報が必要になります。これは初回ログイン後に実行できます。

1. **ISEサーバのIPとログイン情報（ISE Server IP and Credentials）**：Cisco Identify Services Engine（ISE）サーバの IP アドレス、管理ユーザ名、パスワードが必要です。これらは「CISCO ISE と Cisco DNA Center 」で説明されているように、組織の ISE サーバにログインして Cisco DNA Center とのデータ共有設定を行うために必要です。

2. **認証およびポリシーサーバ情報（Authorization and Policy Server Information）**：認証およびポリシーサーバとして Cisco ISE を使用している場合は、上記の ISE の統合と同じ情報に加えて、ISE CLI ユーザ名、CLI パスワード、サーバ FQDN、サブスクライバ名（`cdnac` など）、ISE SSH キー（オプション）、プロトコル選択（RADIUS または TACACS）、認証ポート、アカウンティングポート、および再試行/タイムアウト設定が必要です。

   別の認証およびポリシーサーバを使用している場合は、サーバの IP アドレス、プロトコルの選択（RADIUS または TACACS）、認証ポート、アカウンティングポート、および再試行/タイムアウトの設定が必要になります。

この情報を使用して、選択した認証およびポリシーサーバと Cisco DNA Center を統合します。これについては、「認証サーバとポリシーサーバの設定」で説明しています。

3. **SNMPの再試行とタイムアウト値（SNMP Retry and Timeout Values）**：「SNMP プロパティの設定」で説明されているように、デバイスのポーリングとモニタリングをセットアップするために必要です。